



PATENT ABSTRACTS OF JAPAN

(11) Publication number: 03266544 A

(43) Date of publication of application: 27.11.1991

(51) Int. Cl. H04L 9/32
G09C 1/00(21) Application number: 02066435
(22) Date of filing: 15.03.1990(71) Applicant: NEC CORP
(72) Inventor: NAGASAKA YASUSHI(54) MESSAGE CRYPTOGRAPHIC PROCESSING
AND VERIFICATION SYSTEM

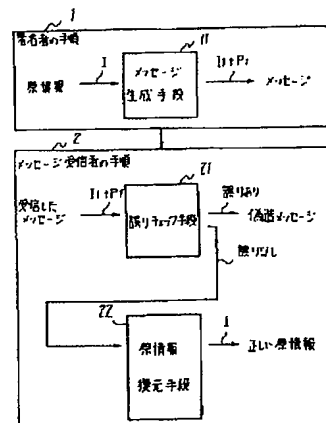
(57) Abstract:

PURPOSE: To reduce a processing time and to attain error check on a communication line by using a generation polynomial for an error check code so as to add a generated identifier thereby forming a cryptographic message.

CONSTITUTION: A signer uses a generation polynomial being a secret key to employ a message generating means 11, which generates a message $I+P1$ resulting from adding an identifier $P1$ to cryptographic information $I1$ resulting from original information I desired to be signed and sends the message to a recipient. The recipient of the message uses an error check means 21 for the sent message $I1+P1$ to check whether or not the received message has a correct error check code thereby identifying whether the message is a correct message or a forgery message. When the error check means 21 discriminates the sent

message to be a correct message, an original information decoding means 22 is used to obtain correct original information I sent by a signer. Thus, the processing time is decreased and the error check on a communication line is attained.

COPYRIGHT: (C)1991,JPO&Japio



⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平3-266544

⑬ Int. Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成3年(1991)11月27日

H 04 L 9/32
G 09 C 1/00

7922-5L
6914-5K

H 04 L 9/00

A

審査請求 未請求 請求項の数 1 (全3頁)

⑮ 発明の名称 メッセージの暗号化および認証方式

⑯ 特 願 平2-66435

⑰ 出 願 平2(1990)3月15日

⑱ 発 明 者 長 坂 康 司 東京都港区芝5丁目33番1号 日本電気株式会社内

⑲ 出 願 人 日本電気株式会社 東京都港区芝5丁目7番1号

⑳ 代 理 人 弁理士 内 原 晋

明 細 書

1. 発明の名称

メッセージの暗号化および認証方式

2. 特許請求の範囲

原情報に対して署名者が認証のための秘密鍵として、署名者特有の誤り検査符号の生成多項式を用いて生成した認証子を付加し、同時にその原情報を前記生成多項式により暗号化したメッセージを作成し、前記メッセージを受信した受信者が受信した前記メッセージに対して、署名者特有の秘密鍵である誤り検査符号の前記生成多項式を適用して復元し、正しい誤り検査符号であった場合にのみ、前記メッセージを正しいメッセージであると認証して復元した原情報を提供することを特徴とするメッセージの暗号化および認証方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明はメッセージの暗号化および認証方式に関し、特にメッセージを暗号化するとともに認証子によりメッセージの認証を行うメッセージの暗号化および認証方式に関する。

〔従来の技術〕

従来のメッセージ^の暗号化および認証方式は、DES(Data Encryption Standard)を用いてメッセージの暗号化とメッセージの認証子とを別々に行っている。

第2図はDESを用いた従来のメッセージの暗号化および認証方式の一例を示すメッセージ構成説明図である。

従来のメッセージの暗号化および認証方式は、第2図に示すように、原情報の64ビットごとに秘密鍵による32ビットの符号をDESで算出し、それらの排他論理和を求めることにより、32ビットの認証子を生成して付加し、次に原情報をDESで暗号化することにより、DES^の暗号化されたメッセージを作成している。

〔発明が解決しようとする課題〕

上述した従来のメッセージの暗号化および認証方式は、DESを用いて、メッセージの暗号化とメッセージの認証とを別々に行っているので、メッセージの暗号化処理およびメッセージの認証子作成処理が複雑で長い処理時間を要するという欠点を有している。

〔課題を解決するための手段〕

本発明のメッセージの暗号化および認証方式は、原情報に対して署名者が認証のための秘密鍵として署名者特有の誤り検査符号の生成多項式を用いて生成した認証子を付加し、同時にその原情報を前記の生成多項式により暗号化したメッセージを作成し、前記メッセージを受信した受信者が受信した前記メッセージに対して、署名者特有の秘密鍵である誤り検査符号の前記生成多項式を適用して復元し、正しい誤り検査符号であった場合にのみ、前記メッセージを正しいメッセージであると認証して復元した原情報を提供することにより構成されている。

〔実施例〕

数である)と表す。

そこで、メッセージ $I1 + P1$ は、 $I(X)$ と $G(X)$ との積の多項式の係数で示す情報として求める。このときメッセージ $I1 + P1$ は、見た目にはどれが情報ビットでどれが検査ビットの判断がつかない情報となる。

なお、生成多項式 $G(X)$ は、署名者と正規の受信者のみが知っている秘密鍵である。

次に、メッセージ受信者の手順2を説明する。

メッセージの受信者は、送信者から送られてきたメッセージ $I1 + P1$ に対して、誤りチェック手段21を用いて、受け取ったメッセージが正しい誤り検査符号であるかどうかをチェックすることにより、正しいメッセージか偽造メッセージかを識別する。すなわち、正しいメッセージか偽造メッセージかを識別するには、受信したメッセージ $I1 + P1$ を秘密鍵である生成多項式 $G(X)$ で割って余りが0であるかどうかをチェックして、余りが0であれば、正しいメッセージと判断し、余りが0でなければ、偽造メッセージと判断する。

次に、本発明の実施例について図面を参照して説明する。第1図は本発明のメッセージの暗号化および認証方式の一実施例を示すブロック図である。

まず、第1図により署名者の手順1を説明する。署名者は秘密鍵である生成多項式によりメッセージ作成手段11を用いて、署名したい情報である原情報 I を暗号化した $I1$ に認証子 $P1$ を付加したメッセージ $I1 + P1$ を作成して、受信者に送信する。

ここで、メッセージ作成手段11におけるメッセージの作成方法を説明する。原情報を

$$I(X) = A_k X^k + A_{k-1} X^{k-1} + \dots + A_1 X + A_0$$

(但し、 k は情報ビット数、 A_i は1または0の情報ビットである)と表し、生成多項式を

$$G(X) = G_{n-k} X^{n-k} + G_{n-k-1} X^{n-k-1} + \dots + G_1 X + G_0$$

($n-k$ は検査ビット数、 G_i は1または0の係

このメカニズムが正しいことは巡回符号である誤り検査符号の性質から容易に証明できる。

そして、誤りチェック手段21により、正しいメッセージであると判断されたならば原情報復元手段22を用いて署名者が送った正しい原情報 I を求める。すなわち、この手順は署名者の手順1の逆であり、受信したメッセージ $I1 + P1$ を秘密鍵である生成多項式で割った結果の商を求めることにより、署名者が送った正しい原情報 I が得られることとなる。

〔発明の効果〕

以上説明したように、本発明のメッセージの暗号化および認証方式は、誤り検出符号の生成多項式を用いることにより、大幅に処理時間が少なくてすむとともに、誤り検査符号を使用しているので通信路上の誤りチェックも可能であるという効果を有している。

4. 図面の簡単な説明

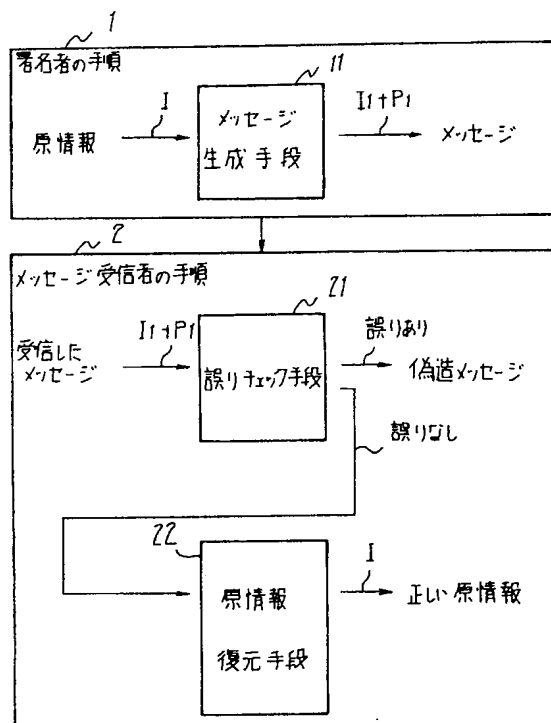
第1図は本発明のメッセージの暗号化および認

証方式の一実施例を示すブロック図、第2図はDESを用いた従来のメッセージの暗号化および認証方式の一例を示すメッセージ構成説明図である。

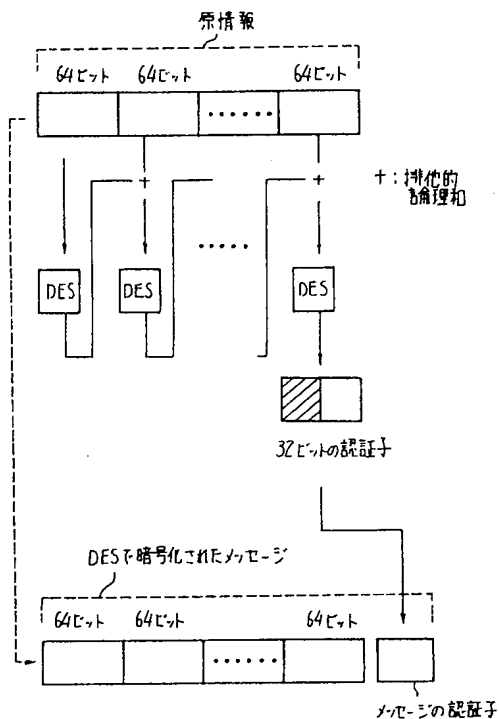
- 1……生成多項式(秘密鍵)により、誤り検査符号を得る手段
 2……生成多項式を用いて誤りチェックを行う手段
 3……受信した誤り検査符号を生成多項式を用いて情報ビットと検査ビットに分離する手段

1……署名者の手順、2……メッセージ受信者の手順、11……メッセージ生成手段、21……誤りチェック手段、22……原情報復元手段、I……原情報、I+P1……メッセージ。

代理人 弁理士 内 原 晋



第 1 図



第 2 図